BY ORDER OF THE GOVERNOR

HQ LA ANG INSTRUCTION 33 - 3

1 APRIL 2003

Communications and Information

159th FIGHTER WING NETWORK SECURITY POLICY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the Headquarters WWW site at: http://hq.mil

OPR: 159CF/SCBS (MSgt Tiffanni L. Beckham)
Supersedes: HQ LA ANGI 33-3, 22 Jan 01

Certified by: 159CF/SCB (CMSgt Elaine P. Vix)
Pages: 9
Distribution: F

This instruction establishes the guidelines and procedures for the proper use of the 159th Fighter Wing (FW) Wide Area Network, hereafter referred to as the network. It was created to ensure that all network computer users have adequate guidance regarding the policies that govern connection to the network and safeguarding information processed on the network. 159th Communications Flight (CF) Information Assurance (IA) personnel created this instruction to document the established policies and operational procedures that ensure the secure use and administration of the network.

SUMMARY OF REVISIONS
This document is substantially revised and must be completely reviewed.

1. Glossary of References and Supporting Information. See Attachment 1.

2. Introduction.

2.1. Mission. The 159 CF is responsible for operating and maintaining data communication systems that support the 159FW, 236CBCS, 122ASOS, 259ATCS, 122WF, 214EIS and HQ LAANG. This allows for internal and external data connectivity to the network and other systems. The network allows for the rapid transmission of data from one service user to another in a sufficiently error-free, reliable and physically secure fashion.

3. Applicability and Scope. This security directive provides the minimum computer security requirements and establishes the set of rules and practices that regulate management, protection and distribution of data entrusted to the network. The provisions contained herein are directive in nature and applicable to all FW and Geographically Separated Units (GSU) personnel authorized to operate an Automated Information System (AIS) supported by the network. Failure to observe its provisions will result in administrative or judicial actions, to include punishment under the Uniform Code of Military Justice and Federal Law.

4. Security Objectives.

4.1. Confidentiality. The security objective of confidentiality shall be factored into all requirements to ensure only authorized personnel with proper clearances and need-to-know are allowed access to network resources and information.

4.2. Availability. The security objective of availability ensures that the network is readily available for use by authorized personnel and connected users when it is needed.

4.3. Integrity. The security objective of integrity ensures that the data processed, stored, or handled by the network shall be accurate and reasonably immune from malicious or unintentional alteration by unauthorized personnel.

5. System Security.

5.1. Restrictions & Limitations. Only official government business should be conducted while operating a government AIS. The following actions are strictly prohibited:

5.1.1. Illegal, fraudulent or malicious activity.

5.1.2. Storing or processing classified information on any system not specifically approved for classified processing.

5.1.3. Using another individuals account or identity, or sharing personal logon ID's and passwords.

5.1.4. Attempting to circumvent or defeat security or auditing systems.

5.1.5. Installing or using files from any source prior to scanning for malicious code or viruses using approved detection software methods.

5.1.6. Modifying, altering or bypassing the operating system or system configuration of an AIS without first obtaining permission from Network Control Center (NCC).

5.2. Access Control.

5.2.1. Identification & Authentication. Identification is the process where individuals identify themselves to a system as a valid user. Authentication is the procedure where the system verifies that the user has a right to access the system. Each control system will enforce individual accountability by requiring unique individual identifiers. The system will use passwords to authenticate the user's identity and privileges. Only NCC personnel shall have modification or deletion rights to these files.

5.2.2. Certification & Accreditation (C&A). Certification validates the security assurance for a system associated with an environment. Accreditation evaluates whether the operational impacts associated with any residual system weaknesses are tolerable or unacceptable. The degree of assurance assumed by the Designated Approving Authority (DAA) ensures the system is able to enforce its security policy. Certification validates the security assurance for a system associated with an environment. Accreditation evaluates whether the operational impacts associated with any residual system weaknesses are tolerable or unacceptable. This package is a living document that shall be reviewed at least annually for accuracy or upon any changes in the configuration of the system that could alter its security posture.

5.3. Network Boundary Security Stance. A base level boundary protection (Barrier Reef) solution is established at the Region 3 Regional Operations Security Center to provide protection from the harmful aspects of the Internet. This stance dictates that network users will only be granted the privileges and access that is required to perform their duties. This solution must allow evolutionary improvements to handle new security threats as they are recognized.

5.4. Remote Dial-Up Access/Virtual Private Network. In order to provide the highest degree of protection to the network, external connections will only be accomplished within the immediate control of the NCC. This will ensure that all external connections can be appropriately controlled and monitored for intrusion. Organizations that do not comply with this policy item may be disconnected from the network. Exceptions to this item will be handled on a case-by-case basis.

5.4.1. Dial-In/Virtual Private Network connections must meet the following requirements. Due to security requirements dial-in access will be granted for government resources only.

5.4.2. The 159FW dial-in/virtual private network procedures will be evaluated routinely to ensure applicable security is in place.

5.4.3. There will be a minimum of two levels of security in place at all times.

5.4.4. Access code(s) and/or passwords will be required to enter the dial-in service.

5.4.5. NT user passwords will be required to access the network.

5.4.6. All passwords will be changed every 90 days.

5.4.7. All requests for dial-in/virtual private network access must be e-mailed to the Helpdesk by **Unit Commanders** only.

5.4.8. All individuals approved for dial-in/ virtual private network access will be removed from access upon completion of the deployment for which access was approved.

5.4.9. No individual will be authorized dial-in/virtual private network access for a period longer than one year.

5.5. Remote Access Via Modem. Telephone dial-up systems, which grant access to the network will be under the control of the NCC. To reduce the inherent risks associated with the use of modems, the following protections are required in accordance with AFI 33-202, *Computer Security*, on all AIS's that employ modems to provide remote access to the network. Non-compliance warrants interface termination.

5.5.1. Security Requirements. These security requirements apply to systems allowed to remotely access the network.

5.5.2. Call-forwarding. Call forwarding is prohibited when call back or dial back technology is used.

5.5.3. Disclosure. Do not publicize modem telephone numbers to anyone other than those with a need-to-know and authorization to use. Telephone numbers shall be protected as For Official Use Only.

5.6. Password Policy. Good password discipline is essential to defend against compromise and loss of information. Passwords must be changed every 90 days. Each user is responsible for adhering to the basic criteria of good password management including password composition and length, life cycle management, ownership, distribution, entry and safeguarding. Users violating this policy endanger will be denied access to the network.

5.6.1. Password Composition. Passwords must consist of at least eight alphanumeric characters (upper and lower case) with at least one special character (# @ *, etc.). Do not use a single word by itself, especially those from the dictionary, slang, names or profanity.

5.6.2. Password Protection. Do not write passwords down or share passwords. Do not leave your workstation or terminal unprotected while you are logged in. If password compromise is suspected, change the password immediately and report the incident to your Workgroup Manager (WGM) or Computer Security (COMPUSEC) Manager.

5.6.3. Password Lockouts. Unsuccessful access attempts shall be limited to three. When network passwords have been locked out, the WGM must contact the Helpdesk via e-mail, to have it reset. When Standard Base Supply System or Core Automated Maintenance System user-ids have been locked-out, the user must contact the Unit Terminal Area Security Officer to have it reset.

5.6.4. Password Disclosure. Users will not disclose their passwords to anyone for any reason, regardless of rank or position of the requesting individual.

5.6.5. Password Monitoring. NCC personnel will routinely monitor password lockouts and will execute password-cracking software to ensure passwords adhere to the applicable password policies listed above and in higher headquarters applicable directives.

5.7. Network Control Center Monitoring. System Administrators (SA) are critical to the maintenance of essential Air Force communications systems and their primary responsibility is to administer the network. When an SA discovers evidence of Fraud, Waste and Abuse (FWA) or other misuse during the course of their normal SA duties, they may access the content of those communications so far as is necessary to confirm FWA or other misuse has occurred. When the incident of FWA has been confirmed, an administrator should report the incident to their supervisor, appropriate commander or Office of Special Investigation as required.

5.8. Internet Access. Access to the Internet through a government computer is provided to conduct official and authorized government business only. Regardless of location, if the account being used is one provided by the United States Government, only official business will be conducted via that access. Using the Internet for other than authorized uses will result in adverse administrative or disciplinary action. All network users will utilize the latest version of Internet Explorer provided by the NCC. Requests to use other browsers may be granted based on the requestors mission justification.

5.9. Electronic Mail (E-Mail). Electronic mail is official communication. E-mail will be used to transmit both formal and informal correspondence. Use formal e-mail to replace or supplement formal Air National Guard formats for communications such as official memorandums, letters, etc. Use informal e-mail to replace or supplement telephone calls, notes or informal communication between individuals. Although informal e-mail is permitted, this does not permit the use of foul language in messages or transmission of chain letters, EXE, MP3, MOV, JPEG, WAV, or MPEG files through the e-mail system. Using e-mail in either of these manners may result in adverse administrative or disciplinary action.

5.10. Outlook Web Access (OWA). OWA is an extension of Microsoft Exchange with the intended purpose of allowing access to e-mail from remote locations. It is to be used with the same discretion and limitations as routine e-mail.

5.11. Mailbox Restrictions. User mailbox restrictions will be enforced to prevent saturation and degradation of the network mail server. When the mailbox has exceeded prescribed limits, the user will receive a warning. Requests to exceed these limits may be approved on an individual basis by the Information Systems Branch Chief. The limits and restrictions are as follows:

5.11.1. 20MB - Messages can be sent and received, but the user should delete all unnecessary messages or move them to personal folders.

5.11.2. 30MB - Messages can be received but none can be sent until the user deletes all unnecessary messages or moves them to personal folders.

5.11.3. 35MB - Messages cannot be sent or received until the user deletes all unnecessary messages or moves them to personal folders.

6. Internet Service Provider (ISP) Restrictions. Email traffic destined for other military sites (within the ".mil" domain) will not be routed through an ISP, and traffic from an ISP will not be routed through the receiving base network to other military networks. Other than the mail service provided by the LAANG (MS Exchange), no other commercial mail service (i.e., AOL, Hotmail, Yahoo, etc.) is authorized. Access to these sites from the LAANG network is prohibited and will be blocked.

7. Personnel Security. Personnel security is defined as the procedures established to ensure all personnel have the appropriate security clearance and need-to-know prior to being granted access to the network.

8. Physical Security.

8.1. Entry Controls to Remote Terminals. Each terminal shall be protected against tampering and theft. Protection will be provided by controlling physical access to the terminal. This will be accomplished by using two levels of physical security, including doors, keyboard locks, etc. For example, during off-duty hours for a person to gain access to a terminal, that person must gain entry through two locked doors before getting to the terminal. Building doors that are locked during off duty hours can serve as one barrier and a locked office door can serve as an additional barrier.

8.2. Resource Protection. All personnel must protect system resources (processors, terminals, communication media, etc.) against natural threats (e.g. flood, weather), physical disasters (e.g. fire), human threats (intentional and unintentional) and any other identified physical threat. All personnel are required to control access to system resources. Positive identification (by personal recognition) is required for persons attempting to access system resources. Personnel should challenge any individual they cannot positively identify. If in doubt, verify the status of the individual. Status implies not only the appropriate clearance and need to access system resources, but that the individual is authorized to perform the function for which access is requested and the function constitutes official business.

9. Unattended System/Screen Saver. If there has been no activity on a computer terminal workstation for 10 minutes, the system will be configured to automatically invoke a password protected screen saver and suspend the session. Re-establishment of the session must take place only after the authorized user or a system administrator has provided a valid password. When a user leaves the area, the terminal/workstation must be logged off, locked or a password protected screen saver must be applied.

10. Malicious Logic (Virus) Protection. All computer systems at the FW and all GSUs will use Norton anti-virus software. Virus scans should be conducted on a regular basis and all files will be scanned prior to downloading to a computer system. Individuals that do not comply with this policy will be denied access to the network.

11. Contingency Planning. Contingency planning ensures that users can continue to perform essential functions in the event the operation of the network is interrupted. This plan shall be consistent with disaster recovery plans maintained by the organization. NCC personnel will develop and maintain plans to ensure the survival and timely recovery of the mission critical and essential systems. The plans shall identify which areas are most vital and the level of protection necessary to ensure mission accomplishment. The plan will be reviewed and selectively tested at least annually by NCC personnel.

12. Marking and Labeling. Appropriate marking/labeling applies to printed listings, display terminals, diskettes/storage jackets and storage devices. Diskettes, back-up tapes, etc. will be labeled according to the classification of the information stored on the media. Labeling should be done using the applicable Standard Form Label: Standard Form 706 – **Top Secret**, Standard Form 707 – **Secret**, Standard Form 708 – **Confidential**, Standard Form 710 – **Unclassified**. Products and media which require special marking and handling such as For Official Use Only shall be marked according to applicable regulations. Products and media which contain sensitive data shall be locked up when not in use and cleared from the network when no longer needed. All equipment will be processed through the Base Equipment Control Officer and added to the proper Information Processing Management System account. Bar code labels will be physically applied to equipment when applicable. All floppy disks and CD-ROMs used to store/backup data should be marked using the appropriate classification label.

13. Configuration Management. The Network Manager (NM) will maintain control of all network configuration issues. Changes which could affect the security baseline of the Network must be approved by the DAA. The following items require configuration control; identification of new/changed requirements, software updates, hardware changes, changes to system security default parameters, test scenarios and changes to documentation.

14. Declassification/Destruction. In the event that information above the approved level of classification is processed on the Network, it is imperative that the user contacts the NM and Wing Information Assurance Office as soon as possible. The users terminal and any other involved devices will be completely disconnected from the Network. Destruction of the media and any output will be conducted in accordance with AFSSI 5020, *Remanence Security.*

15. Copyrighted Software. Only government produced and legally procured software shall be used on government AISs. No software will be downloaded or otherwise procured from a bulletin board system, public or private software repository of any kind, or from any Internet source without prior NCC approval. This includes shareware, freeware, and public domain software. Only legal copies of copyrighted software will be used. Questions regarding copyright issues should be directed to the NCC for resolution.

16. Civilian Network Access. All civilian employees requiring access to the base network must coordinate access with the Unit WGM. They must possess at least a National Agency Check verified by the employing agency security manager. The civilian employee must also present a Visit Authorization Letter (VAL) upon arrival to the Unit WGM which lists the individuals name, social security number, security clearance, and duration of visit. The VAL should be created and signed by the employing agency security manager. The Unit WGM must ensure that the civilian employee completes the Information Awareness Computer Based Training located on the 159th Fighter Wing intranet webpage.

17. Roles and Responsibilities.

17.1. Designated Approving Authority. The DAA accredits all AISs under their jurisdiction prior to their operation. Through accreditation, the DAA formerly accepts responsibility for the secure operation of the system to operate in specific environment. The DAA is responsible for approving security requirement documents, the C&A plan, memorandums of agreement, and deviations from the security policy. The DAA ensures certifying officials, functional office of primary responsibility and Computer Systems Security Officers are identified for all AISs under their jurisdiction.

159th Fighter Wing DAA - Col John B. Soileau, Jr.

17.2. Base Communications & Information Systems Officer (CSO). The Base CSO is the host wing communications officer and is appointed by the Wing Commander. The CSO is responsible for meeting the FW and GSU communications and information mission needs. The CSO serves as the accountable officer for computer hardware and software.

159th Fighter Wing Base CSO – Capt Arthur B. Troncoso, III

17.3. Network Control Center. The NCC cooperative team includes network operators who perform Helpdesk (HD) operations, Information Assurance office personnel, and Network Administration personnel. The NCC provides responsive mission support by managing the local Network that provides customers the communications and information resources needed to achieve their operational objectives. It serves as the single focal point for base network management and problem resolution. Communications and information services entering and exiting the network fall under the operational control of the NCC.

17.4. Wing Information Assurance Office. The Wing IA Office oversees the implementation of information protection policy and guidance. This office implements and enforces national, Department of Defense, and Air Force security policies and directives. The Wing IA office also advises the DAA, certifying officials and others involved in network security policy formation.

17.5. Helpdesk Operators. The Helpdesk is the focal point for problem resolution. The HD provides a central repository for technical advice and solutions for network systems, software applications assistance, automatic data processing support, hardware exchange, and repair service support. The HD determines the type of reported system problem, reports the status of problem resolution to the affected customer, and maintains a historical database of problem resolution.

17.6. Network Administration Office. The Network Administration Office provides proactive and reactive network management by monitoring and controlling the network, available bandwidth, hardware and software resources.

17.7. Workgroup Manager/Unit Computer Security (COMPUSEC) Manager. The WGM is the individual operationally and administratively responsible for the mission of the AIS. This individual serves as the primary point-of-contact between users in their area of assignment and the 159CF for obtaining technical assistance. They establish and administer the computer security program for their units. They are responsible for reviewing and approving AIS security safeguards, reviewing risk analyses, and certifying that AISs under their control meet security requirements. WGMs are additionally responsible for obtaining accreditation for all AISs in their control prior to operational use and requesting network passwords or user-ids. They resolve the daily problems users experience and contact the HD if the problem cannot be resolved at the unit level. They ensure that all personnel comply with established security policies.

17.8. Network Users. Each user of an AIS connected to the network shall comply with the provisions set forth in this policy.

18. Forms Prescribed. Standard Form 706, **Top Secret (Label)**, Standard Form 707, **Secret (label)**, Standard Form 708, **Confidential (Label)**, and Standard Form 710, **Unclassified (Label)**.

BY ORDER OF THE GOVERNOR

BENNETT C. LANDRENEAU
Major General, LAARNG
The Adjutant General

OFFICIAL

//Signed//

JOHN B. SOILEAU, JR., COL, LA ANG
Acting ESSO

Attachment:
Glossary of References and Supporting Information

Attachment 1

Glossary of References and Supporting Information

References

AFI 31-401, *Information Security Program Management*
AFI 31-501, *Personnel Security Program Management*
AFI 33-115 VI, *Network Management*
AFI 33-119, *Electronic Mail (E-Mail) Management and Use*
AFI 33-202, *Computer Security*
AFI 33-204, *Information Assurance (IA) Awareness Program*
AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*
AFMAN 33-223, *Identification and Authentication*
AFSSI 5020, *Remanence Security*
AFSSI 5023, *Viruses and Other Forms of Malicious Logic*
AFSSI 5024 VI, *The Certification and Accreditation Process*
AFSSI 5027, *Network Security Policy*
DOD 5200.1-R, *Information Security Program*
159FWI 33-1, *Intranet/Internet Policy*
HQ LA ANGI 33-1, *Network Management*

Abbreviations and Acronyms

AIS - Automated Information Systems
C&A - Certification & Accreditation
CF – Communications Flight
COMPUSEC- Computer Security
CSO - Communications & Information Systems Officer
DAA- Designated Approving Authority
E-Mail- Electronic Mail
FWA – Fraud, Waste, and Abuse
FW - Fighter Wing
GSU- Geographically Separated Unit
HD- Help Desk
IA- Information Assurance
ISP – Internet Service Provider
NCC – Network Control Center
NM – Network Manager
OWA – Outlook Web Access
SA – System Administrators
VAL – Visit Authorization Letter
WGM – Workgroup Manager